Fall 1999

The word problem and the ideal membership problem

Damon Anthony Demas
University of New Hampshire, Durham

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI®

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

The Word Problem and The Ideal Membership Problem

BY

Damon A. Demas

B.A., Cornell University (1992)
M.S., University of New Hampshire (1996)

DISSERTATION

Submitted to the University of New Hampshire
in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

in

Mathematics

September 1999

This dissertation has been examined and approved.

Dissertation director, Edward K. Hinson
Associate Professor of Mathematics

Kenneth I. Appel
Professor of Mathematics

Karen Graham
Associate Professor of Mathematics

Don Hadwin
Professor of Mathematics

Eric Nordgren
Professor of Mathematics

July 20, 1999
Date

Dedication

To friends and family.

Acknowledgments

I am grateful to the graduate school of the University of New Hampshire, for supporting me with a Dissertation Year Fellowship for the academic year 1998 - 1999.

I would like to acknowledge the people who work every day to make the world a better place to be. More specifically, I would like to thank the people who have helped to make my graduate school experience as good as it has been:

Edward Hinson, for being the ideal (pun intended) advisor,

my committee, for their support and reading of my dissertation,

the staff, students, and faculty of the University of New Hampshire mathematics department, and

my friends and family.

Thanks, y'all!!!

Table of Contents

ABSTRACT

The Word Problem and The Ideal Membership Problem

by

Damon A. Demas
University of New Hampshire, September, 1999

This dissertation concerns two problems from computational algebra, the *word problem* for semigroups and the *ideal membership problem* for noncommutative polynomial rings. Historically, the word problem provided one of the first examples of an algorithmically unsolvable problem from outside of logic and computability theory. In terms of solvability, the word problem is equivalent to a restricted version of the membership problem.

For ideals whose membership problem is solvable, computational techniques such as Grobner basis methods often can be used to solve the problem, but not always. In Chapter two, we develop a method which can be used to solve the membership problem for every ideal of a certain class whose membership problem is solvable. In addition, we obtain useful characterizations of those semigroups having a solvable word problem and certain finitely generated ideals having a solvable membership problem. This characterization is extended to a larger class of ideals in Chapter three. Finally, we investigate the word problem for one-relator semigroups in Chapter four. In particular, we show that if there is a one-relator semigroup having an unsolvable word problem, then there is such a semigroup M satisfying (1) the defining relation for M must satisfy certain restrictions concerning the number of occurences of each generator, and (2) the problem of determining whether or not two words having the same number of occurences of each generator are equivalent in M is not solvable.

Chapter 1

Introduction

The main characters of this dissertation are the *semigroup word problem* and the *ideal membership problem.* These are briefly introduced in Sections 1 and 2 of this chapter. In terms of solvability, it is known that the word problem is equivalent to a restricted version of the membership problem. This relationship between the two main characters is investigated through a graph-theoretic lens in Section 3.

1.1 THE SEMIGROUP WORD PROBLEM

Let $\langle x_1, \ldots, x_n \rangle$ denote the free semigroup on n generators. An element X_α of $\langle x_1, \ldots, x_n \rangle$ is called a *word.* Now suppose P is a semigroup generated by $\{x_1, \ldots, x_n\}$. Denote by R the set $\{(a,b) \in \langle x_1, \ldots, x_n \rangle^2 | a = b \text{ in } P\}$. R satisfies the following :

A1. $(a,a) \in R \; \forall \; a \in G$.

A2. $(a,b) \in R \Rightarrow (b,a) \in R$.

A3. $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$.

(R is an equivalence relation), and

A4. $(a,b) \in R, l, r \in \langle G \rangle \Rightarrow (lar, lbr) \in R$.

(R is multiplicative).

If there is a subset R_0 of R such that every element of R follows from R_0 through a finite sequence of applications of (A1) - (A4), then $\langle x_1, \ldots, x_n | R_O \rangle$ is a *presentation* of P. In this case, R is the smallest (with respect to $\subseteq$) equivalence relation on $\langle x_1, \ldots, x_n \rangle$ that satisfies (A4) and contains R_0. If P admits a presentation $\langle x_1, \ldots, x_n | R_0 \rangle$ such that R_0 is finite, then P is a *finitely presented* semigroup, since both the generator set $\{x_1, \ldots, x_n\}$ and the relator set R_0 are finite.

On the other hand, starting with a finite presentation $\langle G | R_0 \rangle$ we obtain a semigroup whose elements are the equivalence classes of elements of $\langle G \rangle$ under the smallest multiplicative equivalence relation on $\langle G \rangle$ containing R_0, and whose operation is defined by concatenation of equivalence class representatives: $[w_1][w_2] = [w_1 w_2]$. The empty word is denoted by 1, and [1] is the identity element under this operation. Given a finite set $S = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$ of pairs of words, let $\mathbf{M_S}$ denote the finitely presented semigroup given by the generating set $G = \{x_1, \ldots, x_n\}$, and the relator set $R_0 = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$.

Word problem for $\mathbf{M_S}$.

INSTANCE: $(X_\alpha, X_\beta) \in \langle x_1, \ldots, x_n \rangle^2$.

PROBLEM: Determine whether $[X_\alpha] = [X_\beta]$ in $\mathbf{M_S}$.

$\mathbf{M}_S$ is said to have *solvable word problem* (resp. *unsolvable word problem*) if there exists (resp. does not exist) an algorithm which solves every instance of the word problem for $\mathbf{M_S}$. By *algorithm* we mean a mechanistic process (such as a Turing machine) which is

guaranteed to terminate in finite time, as opposed to a *procedure*, which may or may not terminate.

The word problem for *groups* was first posed by Max Dehn [7, 8] in 1911. A few years later, the word problem for semigroups was formulated by Axel Thue [24] in 1914, using the terminology of what are now called *Thue systems*. At the time, questions of solvability were not yet an issue for the mathematical mainstream, since the existence of algorithmically unsolvable problems had not yet been established. To quote from [14]:

"Dehn and Thue posed their problems in the positive sense: **find** *a method which would allow determining whether the words are equivalent or not.*

The situation changed in the middle of the 30's with the development of a rigorous **general** *notion of algorithm and Church's Thesis. These achievements, together with the first examples of algorithmically undecidable problems, formed a basis for tackling Dehn's and Thue's problems in the negative direction."*

Now at least the possibility of an unsolvable word problem had to be recognized. Initially, however, conventional wisdom still held that this was not a likely possibility. Quoting from [3]:

"Most of the mathematical community in the 1940's and 1950's regarded unsolvability results as peculiar quirks of logic. They realized that Hilbert's program to provide solutions to all questions that could be stated in a formal system was destroyed but were sure that no problem of interest to them was related to this "horrible" phenomenon".

The semigroup word problem has established its place in history as the needle which would eventually burst this bubble - in 1947, Markov [12] and Post [21] independently proved the existence of a semigroup with unsolvable word problem. Quoting from [14] again,

"Thue's problem was the first decision problem which arose in mathematics proper (i.e., not in logic or calculability theory) and which was shown algorithmically undecidable".

If we are to regard undecidability as a "horrible" phenomenon, then one might hope that examples of semigroups having an unsolvable word problem are themselves horribly complex and unlikely to come up in the course of daily life. Indeed, considerable attention has been given in to trying to determine whether or not semigroups having presentations involving few relators must have solvable word problem.

Matiyasevich [13] showed an example of a three-relator semigroup having unsolvable word problem, but the question of whether or not there exists a semigroup having fewer than three relators and an unsolvable word problem is still open as of this writing. There is optimism that every one-relator semigroup has solvable word problem, in light of W. Magnus' proof [11] that the analogous result for groups is solvable. See [10, 14] for surveys of results on the word problem for semigroups with few relators.

1.2 THE IDEAL MEMBERSHIP PROBLEM

Terminology. Let k denote an arbitrary field, $\langle x_1, \ldots, x_n \rangle$ the free semigroup on n generators, and $k\langle x_1, \ldots, x_n \rangle$ the free k-algebra over $\langle x_1, \ldots, x_n \rangle$. A *monomial* is an element X_α of $\langle x_1, \ldots, x_n \rangle$, a *term* is a product cX_α where $c \in k, X_\alpha \in \langle x_1, \ldots, x_n \rangle$, a *polynomial* is a finite sum $f = c_1 X_{\alpha_1} + \cdots + c_m X_{\alpha_m}$ of terms, and a *binomial* is a sum $c_1 X_{\alpha_1} + c_2 X_{\alpha_2}$ of two terms. ∎

Suppose $\mathbf{I}$ is an ideal in $k\langle x_1, \ldots, x_n\rangle$. The following is a basic problem in computational algebra.

Membership Problem for I.

INSTANCE: $f \in k\langle x_1, \ldots, x_n\rangle$.

PROBLEM: Determine whether or not $f \in \mathbf{I}$.

The ideal I is said to have *solvable membership problem* if there is an algorithm which solves each instance of the membership problem for $\mathbf{I}$. Much of this dissertation is concerned with finding a class of ideals $\mathcal{I}$ for which there is a useful characterization of those ideals of $\mathcal{I}$ having a solvable membership problem. Initially, we will restrict our attention to a very specific class of ideals, before branching out in chapter three. Specifically, let $\mathbf{S} = \{(X_{\alpha_1}, X_{\beta_1}), \ldots (X_{\alpha_t}, X_{\beta_t})\}$ be a finite subset of $\langle x_1, \ldots, x_n\rangle^2$, and let

$$\mathbf{I_S} = (X_{\alpha_1} - X_{\beta_1}, \ldots, X_{\alpha_t} - X_{\beta_t}) \subseteq k\langle x_1, \ldots, x_n\rangle.$$

The membership problem for the ideals $\mathbf{I_S}$ is discussed in Chapter two. In Chapter three we consider the membership problem for a more general class of finitely generated ideals.

The membership problem has been extensively studied in the context of the *commutative* polynomial ring. In the commutative setting, the membership problem for each finitely generated ideal $\mathbf{I}$ can be solved by a standard *Grobner basis* procedure (i.e., compute a finite Grobner basis with respect to an effective term order, and use the division algorithm).

In the noncommutative setting, solving the membership problem is not as straightfor-

ward. In the first place, not every ideal has a solvable membership problem (this follows from the existence of semigroups with unsolvable word problem and the relationship between the the word problem and the membership problem detailed in Section 1.3). Secondly, even if we restrict our attention to those ideals whose membership problem *is* solvable, there are still ideals whose membership problem is not solvable by the Grobner basis procedure mentioned above, as was first shown by Squier [23], and later in [9]. For more on the membership problem in the noncommutative polynomial ring, see [15, 16, 17, 22].

1.3 THE RELATIONSHIP BETWEEN THE WORD AND MEMBERSHIP PROBLEMS

The following notation and terminology will be used throughout the rest of this document. In the semigroup setting, elements of $\langle x_1, \ldots, x_n \rangle$ are called *words.* In the setting of the free k-algebra over $\langle x_1, \ldots, x_n \rangle$, k a field, elements of $\langle x_1, \ldots, x_n \rangle$ are called *monomials.* In the following, "word" and "monomial" are used interchangeably. $\mathbf{S}$ will always denote the finite set $\{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$, where $X_{\alpha_i}, X_{\beta_i}$ are words, and k will always denote an arbitrary field. ∎

The set $\mathbf{S}$ gives rise to the following algebraic structures on $\langle x_1, \ldots, x_n \rangle$:

$\mathbf{M_S}$ - the finitely presented semigroup $\langle x_1, \ldots, x_n | X_{\alpha_1} = X_{\beta_1}, \ldots X_{\alpha_t} = X_{\beta_t} \rangle$.

$\mathbf{I_S}$ - the finitely generated ideal $(X_{\alpha_1} - X_{\beta_1}, \ldots, X_{\alpha_t} - X_{\beta_t}) \subseteq k\langle x_1, \ldots x_n \rangle$.

The graph $\mathbf{G_S}$

To aid in investigating the connections between $\mathbf{M_S}$ and $\mathbf{I_S}$, we introduce a graph $\mathbf{G_S}$ with vertex set $V(\mathbf{G_S}) = \langle x_1, \ldots x_n \rangle$, and an edge between the vertices X_α and X_β if and only if there is an integer $i, 1 \leq i \leq t$, and monomials L and R such that $X_\alpha = LX_{\alpha_i}R, X_\beta = LX_{\beta_i}R$. Thus a *path* in $\mathbf{G_S}$ is an l-tuple $p = (p_1, \ldots, p_l)$ of monomials ($l \in \mathbf{N}$) such that p_i is adjacent to p_{i+1} in $\mathbf{G_S}$ (i.e., there is an edge from p_i to p_{i+1} in $\mathbf{G_S}$), for $1 \leq i \leq l-1$. The origin and terminus of the path p are defined by $o(p) = p_1$ and $t(p) = p_l$. For $X_\alpha \in \langle x_1, \ldots, x_n \rangle$, let $C_S(X_\alpha)$ denote the connected component of X_α in $\mathbf{G_S}$. Similar structures have been studied in [4], [5], and [19].

Example. Write x for x_1, y for x_2, and let $\mathbf{S} = \{(xyx, yy)\}$. Consider the words $X_\alpha = yyyx$ and $X_\beta = xyyy$. We have:

1. $C_S(X_\alpha) = C_S(X_\beta)$, since both X_α and X_β are adjacent to $xyxyx$ in $\mathbf{G_S}$.

2. $X_\alpha = X_\beta$ in $\mathbf{M_S}$, since $yyyx = xyxyx = xyyy$ in $\mathbf{M_S}$.

3. $X_\alpha - X_\beta \in \mathbf{I_S}$, since both $yyyx - xyxyx$ and $xyxyx - xyyy$ are in $\mathbf{I_S}$, and hence their sum is in $\mathbf{I_S}$.

Theorem 1.1 *Suppose $X_\alpha, X_\beta \in \langle x_1, \ldots, x_n \rangle$. The following are equivalent:*

1. $C_S(X_\alpha) = C_S(X_\beta)$.

2. $X_\alpha = X_\beta$ *in* $\mathbf{M_S}$.

3. $X_\alpha - X_\beta \in \mathbf{I_S}$.

Proof.

$2 \Rightarrow 1$. Let $R = \{(a,b) | a = b \text{ in } \mathbf{M_S}\}$ and let $\mathcal{T} = \{(a,b) | C_S(a) = C_S(b)\}$. It suffices to show that $R \subseteq \mathcal{T}$. Since R is the smallest relation on the monomials containing S and

satisfying conditions (A1) - (A4) of Section 1.1, we need only show that $\mathcal{T}$ satisfies (A1) -(A4) and that $\mathcal{T}$ contains S. Each of these is easily verifiable, and left to the reader.

$1 \Rightarrow 3$. Suppose X_α and X_β are in the same connected component of $\mathbf{G}_S$.

If $X_\alpha = X_\beta$, then $X_\alpha - X_\beta = 0 \in \mathbf{I}_S$. Otherwise, there is a path $\mathcal{P}$ in $\mathbf{G}_S$ consisting of distinct vertices $X_\alpha = a_0, a_1, \ldots, a_{n-1}, a_n = X_\beta$ and edges e_i from a_i to a_{i+1} for each $i, 0 \leq i \leq n-1$. Since e_i is an edge in $\mathbf{G}_S$, there exist words l_i, r_i and $j, 1 \leq j \leq t$ such that

(i) $a_i = l_i X_{\alpha_j} r_i$ and $a_{i+1} = l_i X_{\beta_j} r_i$, or

(ii) $a_i = l_i X_{\beta_j} r_i$ and $a_{i+1} = l_i X_{\alpha_j} r_i$.

In either case, $a_i - a_{i+1} \in \mathbf{I}_S$ for $0 \leq i \leq n-1$,, and so

$$X_\alpha - X_\beta = a_0 - a_n = \sum_{i=0}^{n-1} a_i - a_{i+1} \in \mathbf{I}_S.$$

$3 \iff 2$. [18], Theorem 1. ∎

Condition 3 of Theorem 1.1 leads us to consider a restricted version of the membership problem, the *binomial difference membership problem.*

Binomial Difference Membership Problem for I.

INSTANCE: Monomials X_α, X_β

PROBLEM: Determine whether or not $X_\alpha - X_\beta \in \mathbf{I}$.

We will call a graph G *computable* if there is an algorithm which takes as input two vertices v and w from G and determines whether or not v and w are in the same connected

component of G. We are now ready to state Corollary 1.2, which establishes the connection between the word problem and the membership problem.

Corollary 1.2 *For* $S = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$, *the following are equivalent:*

1. $\mathbf{G}_S$ *is computable*
2. $\mathbf{M}_S$ *has solvable word problem*
3. $\mathbf{I}_S$ *has solvable binomial difference membership problem.*

Proof. Since the conditions (1) - (3) of Theorem 1.1 are equivalent, their respective decidabilities are also equivalent. ∎

In Section 4, we will prove the following result:

Theorem 1.3 *The binomial difference membership problem for* $\mathbf{I_S}$ *is solvable if and only if the membership problem for* $\mathbf{I_S}$ *is solvable.*

Thus Corollary 1.2 can be strengthened:

Corollary 1.4 *For* $S = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$, *the following are equivalent:*

1. $\mathbf{G}_S$ *is computable*
2. $\mathbf{M}_S$ *has solvable word problem*
3. $\mathbf{I}_S$ *has solvable membership problem.*

1.4 PROOF OF THEOREM 1.3

Lemma 1.5 *Suppose* $f = c_1X_{\gamma_1} + \cdots + c_mX_{\gamma_m} \in k\langle x_1, \ldots, x_n\rangle$. *Let* $\mathcal{A} = \{A_1, \ldots, A_r\}$ *be a partition of the set* $\{1, \ldots, m\}$ *such that*

$$i \text{ and } j \text{ are in the same cell of } \mathcal{A} \iff C_S(X_{\gamma_i}) = C_S(X_{\gamma_j}),$$

and, for $1 \leq i \leq r$, *let*

$$f_i = \sum_{h \in A_i} c_h X_{\gamma_h}.$$

Then:

$$f \in \mathbf{I_S} \iff f_i \in \mathbf{I_S} \ \forall i, 1 \leq i \leq r.$$

Proof.($\Rightarrow$) Suppose $f \in \mathbf{I_S}$. Then f can be expressed as a linear combination of the generators of $\mathbf{I_S}$,

$$f = \sum_{j=1}^{m} d_j L_j (X_{\alpha_{p_j}} - X_{\beta_{p_j}}) R_j,$$

where $m \in \mathbf{N}$ and $d_j \in k, L_j, R_j \in \langle x_1, \ldots, x_n\rangle, p_j \in \{1, \ldots, t\}$ for $1 \leq j \leq m$. Now let

$$g_i = \sum_{\{j | p_j \in A_i\}} d_j L_j (X_{\alpha_{p_j}} - X_{\beta_{p_j}}) R_j$$

for $1 \leq i \leq r$. Since g_i and f_i are both the sum of the terms of f coming from $\mathcal{A}_i$, we have $g_i = f_i$ for $1 \leq i \leq r$. Clearly $g_i \in \mathbf{I_S}$ for each i, and thus $f_i \in \mathbf{I_S}$ for $1 \leq i \leq r$.

($\Leftarrow$). Suppose $f_i \in \mathbf{I_S}$, for $1 \leq i \leq r$. Then $f \in \mathbf{I_S}$, since $f = f_1 + \cdots + f_r$. ∎

Lemma 1.6 $\mathbf{I_S}$ *contains no monomials.*

Proof. Suppose $f = c_1m_1 + \cdots c_pm_p$ is a polynomial, where $c_i \in k$, and $m_i \in \langle x_1, \ldots, x_n \rangle$ for $1 \leq i \leq p$. Let $C(f)$ denote the sum of the coefficients appearing in f, i.e.:

$$C(c_1m_1 + \cdots + c_pm_p) = c_1 + \cdots + c_p.$$

Now if $f \in \mathbf{I_S}$, f can be expressed as a linear combination of the generators of $\mathbf{I_S}$,

$$f = \sum_{i=1}^{n} c_jL_jX_{\alpha_{p_j}}R_j - c_jL_jX_{\beta_{p_j}}R_j,$$

where $n \in \mathbf{N}$, $c_i \in k, L_j, R_j \in \langle x_1, \ldots, x_n \rangle$, and $p_j \in \{1, \ldots, t\}$ for $1 \leq i \leq n$. Since C is additive and $C(c_jL_jX_{\alpha_j}R_j - c_jL_jX_{\beta_j}R_j) = 0$ for $1 \leq j \leq r$, we have C(f) = 0. Thus f is not a monomial. ∎

Proof of Theorem 1.3. ($\Rightarrow$) Suppose $\mathbf{I_S}$ has solvable binomial difference membership problem and $f = c_1m_1 + \cdots + c_pm_p$ is a polynomial ($c_i \in k, m_i \in \langle x_1, \ldots, x_n \rangle$). Since $\mathbf{I_S}$ has solvable binomial difference membership problem, it is algorithmically possible to write $f = f_1 + \cdots f_r$ where each f_i is comprised of terms all from the same component of $\mathbf{G_S}$, by Theorem 1.1. By Lemma 1.5, then, we may assume without loss of generality that each term of f is from the same component of $\mathbf{G_S}$, i.e.:

$$C_S(m_1) = \cdots = C_S(m_p).$$

If $p = 1$, then $f \notin \mathbf{I_S}$ by Lemma 1.6. If $p > 1$, let $f' = f - (c_pm_p - c_pm_{p-1})$. Now $C_S(m_p) = C_S(m_{p-1})$, so $c_pm_p - c_pm_{p-1} \in \mathbf{I_S}$. Thus $f \in \mathbf{I_S}$ if and only if $f' \in \mathbf{I_S}$. Since f'

has fewer terms than f does, the membership problem for f is solvable by induction on p.

($\Leftarrow$) Clearly if $\mathbf{I_S}$ has solvable membership problem, $\mathbf{I_S}$ has solvable binomial difference membership problem. ∎

Chapter 2

Thorn-free Well-Orderings

One of the standard methods of approaching the membership problem in the noncommutative polynomial ring is with Grobner bases. A rigorous treatment of this approach is given in [16]. Given an ideal $\mathbf{I}$, one attempts to compute a finite Grobner basis for $\mathbf{I}$ with respect to an effective term ordering, and then use the division algorithm to solve the membership problem for $\mathbf{I}$. This method is lacking, however, in that there are ideals $\mathbf{I_S}$ having a membership problem that is solvable, but not solvable by this method [23, 9]. In this chapter, we give a method for solving the membership problem that applies to every ideal of the form $\mathbf{I_S}$ for some $\mathbf{S}$ having solvable membership problem. In the process of doing this, we obtain a useful characterization of those ideals $\mathbf{I_S}$ having a solvable membership problem, as well as analogous results for finitely presented semigroups.

2.1 THORNS

Notation and Terminology. Throughout the rest of this document, S denotes the finite subset$\{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$ of $\langle x_1, \ldots, x_n\rangle^2$, k is an arbitrary field, and $\mathbf{M_S}, \mathbf{I_S}$, and $\mathbf{G_S}$ are as defined in Chapter one. A well-ordering $<$ of the monomials is *sequential* if there is a bijection $a : \mathbf{N} \to \langle x_1, \ldots, x_n\rangle$ such that $a(1) < a(2) < \cdots$. Throughout the rest of this chapter, a will denote such a bijection, and we will write a_n in place of $a(n)$.

A sequential well ordering (swo) $<$ with corresponding bijection a is *effective* if a is a computable function, i.e. if there is an algorithm which, given n, computes a_n. ∎

Fix a swo $<$ with associated bijection a ($a_1 < a_2 < \cdots$). We have seen that, in terms of solvability, the word problem for $\mathbf{M_S}$ and the membership problem for $\mathbf{I_S}$ are equivalent to the problem of characterizing the connected components of $\mathbf{G_S}$:

INSTANCE: $a_k, a_l \in \langle x_1, \ldots, x_n \rangle$.

PROBLEM: Determine whether or not $C_S(a_k) = C_S(a_l)$.

To solve this problem, we need to be able to determine whether or not two monomials a_k and a_l are in the same connected component of $\mathbf{G_S}$. With this in mind, we form the set

$$\mathcal{P}_k = \{\text{cycle - free paths } p \text{ in } \mathbf{G}_S | o(p) = a_k\}.$$

Recall that $o(p)$ denotes the initial vertex of the path p. Our question can now be reformulated: Is there a path $p \in \mathcal{P}_k$ such that $t(p)$ (the terminus of p) is a_l? The set $\mathcal{P}_k$ will not be finite in general, so it is not always possible in finite time to list every element of $\mathcal{P}_k$ and see whether or not its terminus is a_l. Hence we restrict our attention to paths of bounded height, as defined below.

Definition. Suppose $<$ is a sequential well ordering of the monomials with associated bijection a, and $p = (a_{n_1}, \ldots, a_{n_r})$ is a path in $\mathbf{G}_S$. Define the height (with respect to $<$)of p by

$$h_<(p) = \max\{n_i | 1 \leq i \leq r\} - \max\{n_1, n_r\}.$$

Now for $i \in \mathbf{N}$, let

$$\mathcal{P}_{k,i} = \{ \text{ cycle - free paths } p \mid o(p) = a_k \text{ and } h_<(p) < i\}.$$

Since $<$ is sequential, $\mathcal{P}_{k,i}$ is finite for each i, and so the problem of determining whether or not there is a path $p \in \mathcal{P}_{k,i}$ such that t(p) $= a_l$ is thus algorithmically decidable in finite time provided $<$ is effective. Thus, if $<$ is effective, Procedure 2.1 below will terminate if (and only if) a_k and a_l are in the same component of $\mathbf{G}_S$.

Path Connectedness Procedure 2.1.

INPUT: $<$ a swo, $a_k, a_l \in \langle x_1, \ldots, x_n \rangle$

OUTPUT: "Yes" if a_k and a_l are in the same component of $\mathbf{G}_S$.

$i = 1$; done := false;

while (not done) **do**

if $\exists p \in \mathcal{P}_{k,i}$ such that $t(p) = a_l$ **then** output "YES", done := true;

else $i := i + 1$;

One would like to be able to modify this procedure so that it:

1) terminates for arbitrary a_k and a_l, and

2) always gives a correct "YES" or "NO" answer upon termination.

Corollary 1.4, together with the undecidability of the semigroup word problem, imply that in general, however, these goals cannot be achieved simultaneously. One of the obstacles to the guaranteed termination of Procedure 2.1 is the potential presence of *thorns*.

Definition. Suppose $<$ is a swo of $\langle x_1, \ldots, x_n \rangle$ and $\mathbf{G}$ is a graph with vertex set $V(\mathbf{G}) = \langle x_1, \ldots, x_n \rangle$. A *$<$-thorn* in $\mathbf{G}$ is a pair $(t_1, t_2) \in \langle x_1, \ldots, x_n \rangle^2$ satisfying:

(i) $C_S(t_1) = C_S(t_2)$, and

(ii) For every path p in $\mathbf{G_S}$ from t_1 to t_2, $h_<(p) > 0$.

A graph $\mathbf{G}$ with vertex set $V(\mathbf{G}) = \langle x_1, \ldots, x_n \rangle$ is *$<$-thorn-free* if $\mathbf{G}$ has no $<$-thorns.

A thorn in this setting is similar to a *peak* studied by D. Collins [6] in the setting of automorphism groups.

Theorem 2.1 *Suppose G is a graph on the monomials. There exists a sequential well ordering of the monomials such that G is $<$-thorn-free.*

Our proof will show that if G has infinitely many components, then there are uncountably many sequential well orderings $<$ such that G is $<$-thorn-free. Choosing $<$ so that $\mathbf{G}_S$ is $<$-thorn-free allows Procedure 2.1. to be simplified substantially:

Procedure 2.2.

INPUT: $<$, a swo s.t. $\mathbf{G}_S$ is $<$-thorn-free, $a_k, a_l \in \mathbf{G}_S$.

OUTPUT: "YES" or "NO" according to whether or not $C_S(a_k) = C_S(a_l)$.

If $\exists p \in \mathcal{P}_{k,0}$ such that terminus$(p) = a_l$ **then** output "YES" **else** output "NO". ∎

What are the obstructions to making Procedure 2.2 into an algorithm? Theorem 2.1 guarantees the existence of a swo $<$ such that $\mathbf{G}_S$ is $<$-thorn-free. There is no guarantee, however, of the existence of an *effective* swo $<$ such that $\mathbf{G}_S$ is $<$-thorn-free. In fact, those sets S for which there is an effective swo $<$ such that $\mathbf{G}_S$ is $<$-thorn-free are precisely those sets S for which $\mathbf{G}_S$ is computable.

Theorem 2.2 *Suppose* $\mathbf{G}$ *is a graph with vertex set the set* $\langle x_1, \ldots, x_n \rangle$ *of monomials. Then there is an effective swo* $<$ *such that* $\mathbf{G}$ *is* $<$*-thorn-free if and only if* $\mathbf{G}$ *is a computable graph.*

Theorem 2.2 establishes that the method of Procedure 2.2 can be applied to the membership problem for the any of the binomial ideals $\mathbf{I_S}$ having a solvable membership problem.

Corollary 2.3 *For* $S = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\}$, *the following are equivalent:*

1. $\mathbf{G_S}$ *is computable.*

2. $\mathbf{M_S}$ *has solvable word problem.*

3. $\mathbf{I_S}$ *has solvable membership problem.*

4. There is an effective sequential well ordering $<$ *of the monomials such that* $\mathbf{G_S}$ *is* $<$*-thorn-free.*

Proof. Corollary 1.6 and Theorem 2.2. ∎

2.2 PROOFS OF THEOREMS 2.1 AND 2.2

Definition. Suppose $\mathbf{G}$ is a graph with $V(\mathbf{G}) = \langle x_1, \ldots, x_n \rangle, v, w \in V(\mathbf{G})$, and $A \subset V(\mathbf{G})$.

1. Let $d(v, w)$ denote the length of the shortest path from v to w in G, if $C(v) = C(w)$, and ∞ otherwise, and define $d(v, A) = \min\{d(v, w) | w \in A\}$.

2. For a $<$-thorn $t = (t_1, t_2)$, define

$$B(t) = \text{Cardinality}(\{v \in G | C(t_1) = C(v) = C(t_2) \text{ and } v < \max_<\{t_1, t_2\}\}).$$

Lemma 2.4 *Suppose G is a graph on the monomials and $<$ is a swo with associated bijection a $(a_1 < a_2 < \cdots)$. For each $n \in \mathbf{N}$, let $A_n = \{a_1, a_2, \ldots, a_{n-1}\}$. Then*

$$G \text{ is } <\text{-thorn-free} \iff d(a_n, A_n) \in \{1, \infty\} \ \forall n \in \mathbf{N}.$$

Proof. ($\Rightarrow$). Suppose G is $<$-thorn-free, $k \in \mathbf{N}$, and $d(a_k, A_k) \neq \infty$. Then there is $i < k$ such that $C(a_i) = C(a_k)$. Since G is $<$-thorn-free, we know (a_i, a_k) is not a $<$-thorn in G. Thus there is a path $\mathcal{P}$ from a_i to a_k in G, all of whose vertices v are such that $v < a_k$. Let w denote the vertex adjacent to a_k in $\mathcal{P}$. Since $w < a_k$, we have $d(a_k, A_k) = 1$.

($\Leftarrow$). Suppose $d(a_n, A_n) \in \{1, \infty\}$ for each $n \in \mathbf{N}$ and $t = (a_i, a_k)$ is a $<$-thorn in G, with $a_i < a_k$. We consider three cases:

Case 1. a_k is not adjacent to any member of A_k.

In this case we have $d(a_k, A_k) > 1$, and also $d(a_k, A_k) < \infty$, since $a_i \in A_k$ and a_i and a_k are from the same component of $\mathbf{G}$. Thus $1 < d(a_k, A_k) < \infty$, contradicting the hypothesis.

Case 2. a_k is adjacent to a member a_j of A_k and $B(t) = 1$.

Now $a_i \in A_k$ and we have a_i adjacent to a_k, since $B(t) = 1$ prevents any path from a_i to a_k having length greater than 1. This is a contradiction to our hypothesis that (a_i, a_k) is a $<$-thorn.

Case 3. a_k is adjacent to a member a_j of A_k and $B(t) > 1$.

We claim that $t' = (a_i, a_j)$ is a $<$-thorn with $B(t') < B(t)$. Suppose by way of contradiction that t' is not a $<$-thorn. Then there is a path $\mathcal{P}$ from a_i to a_j in G all of whose vertices

v satisfy $v < a_k$. The existence of the path $\mathcal{P}'$ in G consisting of the path $\mathcal{P}$ followed by the edge from a_j to a_k contradicts the assumption that (a_i, a_k) is a $<$-thorn in G. Thus t' is a $<$-thorn in G. Also, $B(t') < B(t)$ since $a_j < a_k$.

The proof may now proceed as follows. Starting with t, both Case 1 and Case 2 lead to a contradiction. In Case 3, we obtain a new thorn t', to which one of the three cases now applies. Since the sequence $\{B(t), B(t'), B(t''), \ldots\}$ is strictly decreasing, we are guaranteed to reach Case 1 or Case 2 eventually, thereby obtaining the desired contradiction. ∎

Proof of Theorem 2.1.

Suppose G is a graph on $\langle x_1, \ldots, x_n \rangle$. Enumerate the components of G as $C_1, C_2, \ldots$. For each $i \in \mathbf{N}$, let

$$J(i) = \begin{cases} \{1, 2, \ldots, m\} & \text{if } \mathrm{Card}(C_i) = m < \infty; \\ \mathbf{N} & \text{if } C_i \text{ is infinite;} \\ \phi & \text{if } G \text{ has fewer than } i \text{ components.} \end{cases}$$

For each $i \in \mathbf{N}$, let $\{c_{i,j}\}_{j \in J(i)}$ denote a nonrepetitive sequence of vertices of G such that $\{c_{i,j} | j \in J(i)\} = C_i$ and $d(c_{i,j+1}, \{c_{i,1}, c_{i,2}, \ldots, c_{i,j}\}) = 1$ for each $j \in J(i)$ (i.e., for each $j \in J(i)$ such that $j \neq 1$, there is $k < j$ such that $c_{i,j}$ is adjacent to $c_{i,k}$). The "diagonal " sequence $\{c_{1,1}, c_{1,2}, c_{2,1}, c_{3,1}, c_{2,2}, c_{1,3}, \ldots\}$ (with undefined terms omitted), gives the desired sequential well order, i.e.:

$$c_{1,1} < c_{1,2} < c_{2,1} < c_{3,1} < c_{2,2} < c_{1,3} < \cdots.$$

Let a be the bijection associated with the swo $<$ above. Clearly $d(a_n, A_n) \in \{1, \infty\}$for all $n \in \mathbf{N}$, and thus G is $<$-thorn-free by Lemma 2.4.

Proof of Theorem 2.2

($\Rightarrow$) Suppose $<$ is an effective sequential well ordering of the monomials such that G is $<$-thorn-free. Two words a_k and a_l are in the same component of $\mathbf{G}$ if and only if there is a path p in $\mathbf{G}$ from a_k to a_l, with $h_<(p) = 0$. Thus, when $<$ is used in Algorithm 1.3, correctness is guaranteed.

($\Leftarrow$) Suppose G is computable. Let $<_d$ be an effective swo (for example, the degree lexicographic ordering), and denote by d_1 the minimal element of $<_d$, i.e. $d_1 \leq_d v\ \forall v \in \langle x_1, \ldots, x_n \rangle$. We claim that Algorithm A1 below computes an effective swo $<$ such that G is $<$-thorn-free.

Algorithm A1. Computes the first m terms of an effective, thorn-free ordering $<$ of G.

Initialization

$a_1 := d_1$;

$\mathcal{A}_1 := \{a_1\}$;

$i := 2$;

Main Loop

while $(i \leq m)$ **do**

$a_i := min_{<_d}\{v | d(v, \mathcal{A}_{i-1}) \in \{1, \infty\}\}$;

$\mathcal{A}_i := \mathcal{A}_{i-1} \bigcup \{a_i\}$;

$i := i + 1$; ∎

Let $\mathcal{A} = \bigcup_{i=1}^{\infty} \mathcal{A}_i$. The first order of business is to show that Algorithm A1 does indeed compute an ordering of the monomials, i.e. we need to show that $\langle x_1, \ldots, x_n \rangle \subseteq \mathcal{A}$.

Claim 1. If v is adjacent to w in $\mathbf{G}$, and $w \in \mathcal{A}$, then $v \in \mathcal{A}$.

Proof of Claim 1. Suppose v is adjacent to w and $w \in \mathcal{A}_n$ for some $n \in \mathbf{N}$. Then, for all $k \geq 1$:

$$v \notin \mathcal{A}_{n+k} \Rightarrow d(v, \mathcal{A}_{n+k}) = 1 \Rightarrow a_{n+k+1} \leq_d v.$$

Since the conclusion $a_{n+k+1} \leq_d v$ is true for at most finitely many k, the hypothesis $v \notin \mathcal{A}_{n+k}$ is also true for at most finitely many k, and thus $v \in \mathcal{A}$.

Claim 2. Suppose C is a component of $\mathbf{G}$ and $v = \min_{<_d} C$, the smallest element of C with respect to $<_d$. Then $v \in \mathcal{A}$.

Proof of Claim 2. Suppose $k \geq 2$ and $v \notin \mathcal{A}_{k-1}$. Then:

$$v \notin \mathcal{A}_{k-1} \Rightarrow d(v, \mathcal{A}_{k-1}) = \infty \Rightarrow a_k \leq_d v.$$

The second implication follows from the definition of a_k. Since the conclusion $a_k \leq_d v$ is true for at most finitely many k, the hypothesis $v \notin \mathcal{A}_{k-1}$ is also true for at most finitely many k, and thus $v \in \mathcal{A}$.

Claim 1 and Claim 2 together show that $\langle x_1, \ldots, x_n \rangle = V(\mathbf{G}) \subseteq \mathcal{A}$. Next we need to verify that the so-called 'Algorithm A1' is in fact an effective algorithm. The question of whether or not $d(v, \mathcal{A}_i) \in \{1, \infty\}$ is computable if and only if the questions of whether or not $d(v, \mathcal{A}_i) = 1$ and whether or not $d(v, \mathcal{A}_i) = \infty$ are both computable. The first

question is always computable since the set $\mathcal{A}_i$ is finite for each i, and the second question is computable because G is computable. Thus Algorithm A1 is in fact an algorithm, and $<$ is effective. Finally, G is $<$-thorn-free by Lemma 2.4. ∎

Chapter 3

The Membership Problem in Binomial Ideals

In Chapter two, we studied the membership problem for the ideals $\mathbf{I_S}$. Here we extend the results of Chapter two to encompass the membership problem for a larger class of finitely generated binomial ideals. Again, $\mathbf{S}$ denotes the finite set $\{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\} \subseteq \langle x_1, \ldots, x_n \rangle^2$. For nonzero elements $c_1, \ldots, c_t$ of k, let

$$\mathbf{I_S}(c_1, \ldots, c_t) = (X_{\alpha_1} - c_1 X_{\beta_1}, \ldots, X_{\alpha_t} - c_t X_{\beta_t}) \subseteq k\langle x_1, \ldots, x_n \rangle.$$

In this notation, the ideal $\mathbf{I_S}$ studied in chapters one and two is $\mathbf{I_S}(1, \ldots, 1)$. An ideal $\mathbf{I}$ of $k\langle x_1, \ldots x_n \rangle$ is a *binomial ideal* if there is a generating set for $\mathbf{I}$ consisting entirely of binomials. Our objective in this chapter is to carry over the results from chapter two on $\mathbf{I_S}$ to the binomial ideals $\mathbf{I_S}(c_1, \ldots, c_t)$ in general. In particular, Corollary 2.3 established the equivalence of the following:

1. $\mathbf{G_S}$ is computable.
2. $\mathbf{M_S}$ has solvable word problem.
3. $\mathbf{I_S}$ has solvable membership problem.
4. There is an effective swo $<$ such that $\mathbf{G_S}$ is $<$-thorn-free.

Our goal here is a result (Corollary 3.8) that establishes, for appropriately chosen $\mathbf{S}, c_1, \ldots, c_t$, the equivalence of:

1. $\mathbf{G_S}$ is computable,
2. $\mathbf{M_S}$ has solvable word problem,
3. $\mathbf{I_S}(c_1, \ldots, c_t)$ has solvable membership problem, and
4. There is an effective swo $<$ such that $\mathbf{G_S}$ is $<$-thorn-free.

3.1. GENERALIZING TO BINOMIAL IDEALS

In the beginning, the results we have developed so far pertaining to the ideals $\mathbf{I_S}$ can be extended so as to apply to the ideals $\mathbf{I_S}(c_1, \ldots, c_t)$ in a straightforward manner. In particular, Theorem 3.3 and Corollary 3.4 are similar to Theorem 1.1 and Corollary 1.2. We start with an analogue of Lemma 1.5.

Lemma 3.1 *Suppose* $f = d_1 X_{\gamma_1} + \cdots + d_m X_{\gamma_m} \in k\langle x_1, \ldots, x_n \rangle$. *Let* $\mathcal{A} = \{A_1, \ldots, A_r\}$ *be a partition of the set* $\{1, \ldots, m\}$ *such that*

$$i \text{ and } j \text{ are in the same cell of } \mathcal{A} \iff C_S(X_{\gamma_i}) = C_S(X_{\gamma_j}),$$

and let

$$f_i = \sum_{j \in A_i} d_j X_{\gamma_j}, \text{ for } 1 \leq i \leq r.$$

Then:

$$f \in \mathbf{I_S}(c_1, \ldots, c_t) \iff f_i \in \mathbf{I_S} \ \forall\, i, 1 \leq i \leq r.$$

Proof. The proof is a straightforward adaptation of the proof of Lemma 1.5. ∎

Lemma 3.2 *Suppose v is adjacent to w in $\mathbf{G_S}$. Then, for $c_1, \ldots, c_t \in k$, there is $d \in k$ such that*

$$v - dw \in \mathbf{I_S}(c_1, \ldots, c_t).$$

Proof. Since v is adjacent to w in $\mathbf{G_S}$, there is an integer j and monomials L, R such that

(i) $v = LX_{\alpha_j}R$ and $w = LX_{\beta_j}R$, or

(ii) $v = LX_{\beta_j}R$ and $w = LX_{\alpha_j}R$.

In the first case, we have $v - c_j w = L(X_{\alpha_j} - c_j X_{\beta_j})R \in \mathbf{I_S}(c_1, \ldots c_t)$, and in the second case $v - c_j^{-1}w = c_j^{-1}L(X_{\alpha_j} - c_j X_{\beta_j})R \in \mathbf{I_S}(c_1, \ldots, c_t)$. ∎

Theorem 3.3 *Suppose $X_\alpha, X_\beta \in \langle x_1, \ldots, x_n \rangle$ and $X_\alpha \notin \mathbf{I_S}(c_1, \ldots, c_t)$. The following are equivalent:*

1. $C_S(X_\alpha) = C_S(X_\beta)$.
2. $X_\alpha = X_\beta$ *in* $\mathbf{M_S}$.
3. *There exists* $d \in k - \{0\}$ *such that* $X_\alpha - dX_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$.

Proof. 1 $\iff$ 2 follows from Theorem 1.1.

1 $\Rightarrow$ 3. Suppose $C_S(X_\alpha) = C_S(X_\beta)$. Then there is a path $\mathcal{P} = (p_1, \ldots, p_l)$ from $p_1 = X_\alpha$ to $p_l = X_\beta$ in $\mathbf{G_S}$. For each $i, 1 \leq i \leq l-1$, there is $d_i \in k$ such that $p_i - d_i p_{i+1} \in \mathbf{I_S}(c_1, \ldots, c_t)$, by Lemma 3.2. Letting $d = \prod_{i=1}^{l-1} d_i$, we have:

$$X_\alpha - dX_\beta = (p_1 - d_1 p_2) - d_1(p_2 - d_2 p_3) + \cdots + \left(\prod_{i=1}^{l-2} d_i\right)(p_{l-1} - d_{l-1}p_l) \in \mathbf{I_S}(c_1, \ldots, c_t).$$

$3 \Rightarrow 1$. Suppose $f = X_\alpha - dX_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$ and $C_S(X_\alpha) \neq C_S(X_\beta)$. Then, applying Lemma 3.1, we have $X_\alpha \in \mathbf{I_S}(c_1, \ldots, c_t)$, contradicting our assumption. ∎

Theorem 3.3 has an immediate corollary.

Corollary 3.4 *Suppose* $\mathbf{I_S}(c_1, \ldots, c_t)$ *contains no monomials. The following are equivalent:*

$1'$. $\mathbf{G_S}$ *is computable.*

$2'$. $\mathbf{M_S}$ *has solvable word problem.*

$3'$. *There is an algorithm that, given arbitrary monomials* X_α *and* X_β*, determines whether or not there is* $d \in k - \{0\}$ *such that* $X_\alpha - dX_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$.

$4'$. *There is an effective swo* $<$ *such that* $\mathbf{G_S}$ *is* $<$*-thorn-free.*

Proof. Since the conditions (1) - (3) of Theorem 3.3 are equivalent, their decidability is also equivalent and thus $(1'), (2')$, and $(3')$ are equivalent. The equivalence of $(1')$ and $(4')$ follows from Corollary 2.3. ∎

The proof of Theorem 3.5 below shows that $3'$ is *stronger* than the condition that $\mathbf{I_S}(c_1, \ldots, c_t)$ has solvable membership problem. Thus for ideals $\mathbf{I_S}(c_1, \ldots, c_t)$ which are known to not contain monomials, we have the following:

If there exists an effective swo $<$ *such that* $\mathbf{G_S}$ *is* $<$*-thorn-free, then* $\mathbf{I_S}(c_1, \ldots, c_t)$ *has solvable membership problem.*

Hypothesis (2) of Theorem 3.5 is a sufficient condition under which the converse of the above result is true.

Theorem 3.5 *Suppose* $\mathbf{I_S}(c_1, \ldots, c_t)$ *is a proper ideal of* $k\langle x_1, \ldots, x_n\rangle$ *that contains no monomials and*

(1) k *is finite, or*

(2) there is a computable function $g : \langle x_1, \ldots x_n\rangle^2 \to k$ *such that*

$$C_S(X_\alpha) = C_S(X_\beta) \iff X_\alpha - g(X_\alpha, X_\beta)X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t).$$

Then the equivalent conditions of Corollary 3.4 are satisfied if and only if $\mathbf{I_S}(c_1, \ldots, c_t)$ *has solvable membership problem.*

Proof. ($\Rightarrow$) Suppose $\mathbf{G_S}$ is computable and $f = \sum_{i=1}^{m}(a_i X_{\gamma_i})$ is a polynomial. Since $\mathbf{G_S}$ is computable, it is algorithmically possible to write $f = f_1 + \cdots + f_k$ as in Lemma 3.1. It suffices to solve the membership problem for the case $k = 1$ and then appeal to Lemma 3.1. Thus, we may assume that the monomials X_{γ_i} appearing in f are all from the same component of $\mathbf{G_S}$, i.e.

$$C_S(X_{\gamma_1}) = \cdots = C_S(X_{\gamma_m}).$$

We proceed by induction on m. If $m = 1$, the membership problem for f is solvable, since $\mathbf{I_S}(c_1, \ldots, c_t)$ is a proper ideal containing no monomials. Now assume $m > 1$ and the membership problem is solvable for all polynomials having fewer than m terms. By Theorem 3.3, there is $d \in k$ such that $a_1 X_{\gamma_1} + dX_{\gamma_2} \in \mathbf{I_S}(c_1, \ldots, c_t)$. To stay constructive, we need to mention that the proof of Theorem 3.3 gives an algorithm to find such a d, once we know it exists. Let $f' = f - (a_1 X_{\gamma_1} + dX_{\gamma_2})$. Note that f' has fewer terms than f does, and $f \in \mathbf{I_S}(c_1, \ldots, c_t) \iff f' \in \mathbf{I_S}(c_1, \ldots, c_t)$. Since the membership problem for f' is solvable by the induction hypothesis, the membership problem for f is also solvable.

($\Leftarrow$). Suppose $\mathbf{I_S}(c_1, \ldots, c_t)$ has solvable membership problem, and $X_\alpha, X_\beta \in \langle x_1, \ldots x_n \rangle$. Given $d \in k$, we can decide whether or not $X_\alpha - dX_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$, by hypothesis. If k is finite, then there are only finitely many candidates for such a d, and checking each of these provides an algorithm satisfying 3'. On the other hand, suppose that there is a function g satisfying hypothesis (2) above. Then

$$\exists d \in k - \{0\} \text{such that} X_\alpha - dX_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$$

$$\Longleftrightarrow$$

(Theorem 3.3)

$$C_S(X_\alpha) = C_S(X_\beta)$$

$$\Longleftrightarrow$$

(hypothesis)

$$X_\alpha - g(X_\alpha, X_\beta)X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t).$$

This latter condition is decidable, so 3' is true. ∎

For ideals $\mathbf{I_S}(c_1, \ldots, c_t)$ satisfying (2) and containing no monomials, we have established the equivalence of the following, in analogy with Theorem 1.2:

1. $\mathbf{G_S}$ is computable.
2. $\mathbf{M_S}$ has solvable word problem.
3. $\mathbf{I_S}(c_1, \ldots, c_t)$ has solvable membership problem.
4. There is an effective swo $<$ such that $\mathbf{G_S}$ is $<$-thorn-free.

3.2 CONSTRUCTION OF THE COMPUTABLE FUNCTION

Our next goal is to demonstrate that many familiar ideals are included in the class of ideals containing no monomials and satisfying hypothesis (2) of Theorem 3.5. The first order of business in this regard is the construction of a suitable computable function. Some preliminary notation is necessary.

For $v, w \in \langle x_1, \ldots, x_n \rangle$, let:

$\hat{x}_i(v) :=$ the number of x_i's appearing in v,

$\hat{\mathbf{x}}(v) := [\hat{x}_1(v), \ldots, \hat{x}_n(v)] \in \mathbf{N}^n$, and

$\Delta(v, w) := \hat{\mathbf{x}}(w) - \hat{\mathbf{x}}(v) \in \mathbf{Z}^n$.

For $S = \{(X_{\alpha_1}, X_{\beta_1}), \ldots, (X_{\alpha_t}, X_{\beta_t})\} \subseteq \langle x_1, \ldots, x_n \rangle^2$, let:

$\Delta(S) := [\Delta(X_{\alpha_1}, X_{\beta_1}), \ldots, \Delta(X_{\alpha_t}, X_{\beta_t})] \in (\mathbf{Z}^n)^t$, and

$\mathrm{sp}(S) := \{\mathbf{n} \cdot \Delta(S) | \mathbf{n} \in \mathbf{Z}^t\}$,

where $\mathbf{n} \cdot \Delta(S)$ denotes the product of $\mathbf{n} = [n_1, \ldots, n_t]$ and $\Delta(S)$ given by

$\mathbf{n} \cdot \Delta(S) = \sum_{i=1}^{t} n_i \Delta(X_{\alpha_i}, X_{\beta_i})$.

Finally, for $\mathbf{c} = (c_1, \ldots, c_t) \in k^t$ and $\mathbf{n} = [n_1, \ldots, n_t] \in \mathbf{Z}^t$, let

$\mathbf{c}^{\mathbf{n}} := c_1^{n_1} \cdots c_t^{n_t}$.

Lemma 3.6 *Suppose X_α and X_β are vertices from the same component of $\mathbf{G_S}$. Then there is $\mathbf{n} \in \mathbf{Z}^t$ such that:*

1. $\Delta(X_\alpha, X_\beta) = \mathbf{n} \cdot \Delta(S)$, *and*

2. $X_\alpha - \mathbf{c}^{\mathbf{n}} X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$.

Proof. Suppose $\mathcal{P} = (p_1, \ldots, p_l)$ is a path in $\mathbf{G_S}$, with $p_1 = X_\alpha$ and $p_l = X_\beta$. For $1 \leq j \leq l-1$, define integers e_j and f_j as follows:

$$f_j = \begin{cases} 1, & \text{if } \exists k, L, R \text{ such that } p_j = LX_{\alpha_k}R \text{ and } p_{j+1} = LX_{\beta_k}R; \\ -1, & \text{otherwise.} \end{cases}$$

$$e_j = \begin{cases} \min\{k | \exists L, R \text{ s.t. } p_j = LX_{\alpha_k}R \text{ and } p_{j+1} = LX_{\beta_k}R\}, & \text{if } f_j = 1; \\ \min\{k | \exists L, R \text{ s.t. } p_j = LX_{\beta_k}R \text{ and } p_{j+1} = LX_{\alpha_k}R\}, & \text{if } f_j = -1. \end{cases}$$

Now for $1 \leq j \leq l-1$, we have:

$$\hat{\mathbf{x}}(p_{j+1}) - \hat{\mathbf{x}}(p_j) = f_j \Delta(X_{\alpha_{e_j}}, X_{\beta_{e_j}}), \text{ and}$$

$$p_j - (c_{e_j})^{f_j} p_{j+1} \in \mathbf{I_S}(c_1, \ldots, c_t).$$

Finally, set $n_i = \sum_{\{j | e_j = i\}} f_j$, for $1 \leq i \leq t$ and set $\mathbf{n} = [n_1, \ldots, n_t]$, so

$$\sum_{j=1}^{l-1} f_j \Delta(X_{\alpha_{e_j}}, X_{\beta_{e_j}}) = \sum_{i=1}^{t} n_i \Delta(X_{\alpha_i}, X_{\beta_i}) = \mathbf{n} \cdot \Delta(S), \text{ and}$$

$$\prod_{j=1}^{l-1} c_{e_j}^{f_j} = \prod_{i=1}^{t} c_i^{n_i} = \mathbf{c}^{\mathbf{n}}.$$

Thus

$$\hat{\mathbf{x}}(X_\beta) - \hat{\mathbf{x}}(X_\alpha) = \hat{\mathbf{x}}(p_l) - \hat{\mathbf{x}}(p_1) = \sum_{j=1}^{l-1} (\hat{\mathbf{x}}(p_{j+1}) - \hat{\mathbf{x}}(p_j))$$

$$= \sum_{j=1}^{l-1} (f_j \Delta(X_{\alpha_{e_j}}, X_{\beta_{e_j}})) = \sum_{i=1}^{t} n_i \Delta(X_{\alpha_i}, X_{\beta_i}) = \mathbf{n} \cdot \Delta(S), \text{ and}$$

$$X_\alpha - (\mathbf{c^n})X_\beta = X_\alpha - (\prod_{j=1}^{l-1} c_{e_j}^{f_j})X_\beta =$$

$$\left(p_1 - (c_{e_1})^{f_1} p_2\right) + \left((c_{e_1})^{f_1} p_2 - (c_{e_2})^{f_2} (c_{e_1})^{f_1} p_3\right) + \cdots + \left(\left(\prod_{j=1}^{l-2} c_{e_j}^{f_j}\right) p_{l-1} - \left(\prod_{j=1}^{l-1} c_{e_j}^{f_j}\right) p_l\right)$$

$\in \mathbf{I_S}(c_1, \ldots, c_t)$. ∎

Example. It is probably worthwhile to work through the notation of Lemma 3.6 in a specific example. Write x for x_1, y for x_2, and let $X_{\alpha_1} = y, X_{\beta_1} = xyx, X_{\alpha_2} = xx$, $X_{\beta_2} = xxy$, and $X_\alpha = xx, X_\beta = xxxx$. Now $S = \{(y, xyx), (xx, xxy)\}$, and for $c_1, c_2 \in k$, $\mathbf{I_S}(c_1, c_2) = (y - c_1xyx, xx - c_2xxy) \subseteq k\langle x, y\rangle$. Furthermore,

$$\Delta(X_{\alpha_i}, X_{\beta_1}) = \hat{\mathbf{x}}(xyx) - \hat{\mathbf{x}}(y) = [2,1] - [0,1] = [2,0], \text{ and}$$

$$\Delta(X_{\alpha_2}, X_{\beta_2}) = \hat{\mathbf{x}}(xxy) - \hat{\mathbf{x}}(xx) = [2,1] - [2,0] = [0,1].$$

Consider the following path $\mathcal{P} = (p_1, p_2, p_3, p_4)$ from X_α to X_β in $\mathbf{G_S}$:

$$xx \longrightarrow xxy \longrightarrow xxyx \longleftarrow xxxx$$

Here $v \longrightarrow w$ means v is adjacent to w and, in particular, w is obtained from v by replacing an X_{α_i} occurring in v by X_{β_i} for some $i \in \{1, 2\}$. We have:

$$f_1 = 1 \quad f_2 = 1 \quad f_3 = -1$$

$$e_1 = 2 \quad e_2 = 1 \quad e_3 = 2.$$

Let $\mathbf{n} = [1, 0]$. We have:

$$\Delta(X_\alpha, X_\beta) = \hat{\mathbf{x}}(X_\beta) - \hat{\mathbf{x}}(X_\alpha) = \sum_{j=1}^{3} f_j u_{e_j} = u_2 + u_1 - u_2 = u_1 = \mathbf{n}\cdot\Delta(S).$$

Also, corresponding to the three edges in $\mathcal{P}$ are three binomials in $\mathbf{I_S}(c_1, c_2)$: $xx - c_2xxy, c_2xxy - c_1c_2xxxyx$, and $c_1c_2xxxyx - c_2^{-1}c_1c_2xxxx$. Their sum, $X_\alpha - \mathbf{c}^{\mathbf{n}}X_\beta (= xx - c_1xxxx)$, is also in $\mathbf{I_S}(c_1, c_2)$. ∎

If X_α and X_β are from the same component of $\mathbf{G_S}$, then $\Delta(X_\alpha, X_\beta) = \mathbf{n}\cdot\Delta(S)$ for some (not necessarily unique!) choice of $\mathbf{n} \in \mathbf{Z}^t$. While $\mathbf{n}$ is not necessarily unique, it is not difficult to make a natural choice for $\mathbf{n}$:

Definition. Suppose $\prec$ is an effective sequential well ordering of $\mathbf{Z}^t$. For $X_\alpha, X_\beta \in \langle x_1, \ldots, x_n\rangle$ such that $\Delta(X_\alpha, X_\beta) \in \text{sp}(\mathbf{S})$, let

$$n_{\prec,S}(X_\alpha, X_\beta) = \min_{\prec}\{\mathbf{n} \in \mathbf{Z}^t | \mathbf{n}\cdot\Delta(\mathbf{S}) = \Delta(X_\alpha, X_\beta)\}.$$

We are now ready to construct the 'suitable computable function' referred to at the end of Section 3.1.

Definition. Suppose $X_\alpha, X_\beta \in \langle x_1, \ldots, x_n\rangle$ and $\prec$ is an effective sequential well ordering of $\mathbf{Z}^t$. Let

$$\mathbf{g}_{\prec,S}(X_\alpha, X_\beta) = \begin{cases} \mathbf{c}^{n_{\prec,S}(X_\alpha, X_\beta)} & \text{if } \Delta(X_\alpha, X_\beta) \in \text{sp}(\mathbf{S}); \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

For the sake of clarity of the exposition, $\mathbf{g}_{\prec,S}$ will sometimes be abbreviated to $\mathbf{g}_{\prec}$.

3.3. BINOMIAL IDEALS WHOSE MEMBERSHIP PROBLEM IS EQUIVALENT TO A WORD PROBLEM

Having constructed $\mathbf{g}_{\prec,S}$, we can now make use of it to show that the hypothesis (2) of Theorem 3.5 is met for certain ideals $\mathbf{I_S}(c_1,\ldots,c_t)$.

Theorem 3.7 *Suppose* $S = \{(X_{\alpha_1}, X_{\beta_1}),\ldots,(X_{\alpha_t}, X_{\beta_t})\} \subseteq \langle x_1,\ldots,x_n\rangle^2$ *and* $\mathbf{c} = (c_1,\ldots,c_t) \in k^t$. *If, for each t-tuple* $\mathbf{a} = [a_1,\ldots,a_t]$ *of integers satisfying* $\mathbf{a}\cdot\Delta(S) = \mathbf{0}$, *we have*

$$\mathbf{c}^{\mathbf{a}} = c_1^{a_1}\cdots c_t^{a_t} = 1, \text{ then:}$$

1. $\mathbf{I_S}(c_1,\ldots,c_t)$ *contains no monomials, and*
2. *For any effective well ordering* $\prec$ *of* $\mathbf{Z}^t$,

$$C_S(X_\alpha) = C_S(X_\beta) \iff X_\alpha - \mathbf{g}_{\prec,S}(X_\alpha, X_\beta)X_\beta \in \mathbf{I_S}(c_1,\ldots,c_t).$$

Corollary 3.8 *For* $\mathbf{I_S}(c_1,\ldots,c_t)$ *satisfying the hypothesis of Theorem 3.7, the following are equivalent:*

1. $\mathbf{G_S}$ *is computable*
2. $\mathbf{M_S}$ *has solvable word problem*
3. $\mathbf{I_S}(c_1,\ldots,c_t)$ *has solvable membership problem.*
4. *There is an effective sequential well ordering* $<$ *of the monomials such that* $\mathbf{G_S}$ *is* $<$*-thorn-free.*

Proof. Theorem 3.5 and Theorem 3.7. ∎

Remark: The hypothesis of Theorem 3.7 is satisfied for:

1. Ideals $\mathbf{I_S}(c_1, \ldots, c_t)$ such that Cardinality(S) $= 1$ and $\Delta(S) \neq \mathbf{0}$. It is also worth mentioning that if Cardinality(S) $= 1$ and $\Delta(S) = \mathbf{0}$, then $\mathbf{I_S}(c_1, \ldots, c_t)$ is a homogeneous ideal and thus is known to have a solvable membership problem [16, p. 159].

2. The ideals $\mathbf{I_S}$. In this case, $c_i = 1$ for each i.

3. Ideals such that $\{\Delta(X_{\alpha_1}, X_{\beta_1}), \ldots, \Delta(X_{\alpha_t}, X_{\beta_t})\}$ is linearly independent over $\mathbf{Z}$. In this case, $a_i = 0$ for each i.

3.4 PROOF OF THEOREM 3.7

We first make a useful definition. Suppose f is a $k(x_1, \ldots, x_n)$-linear combination of the generators $X_{\alpha_1} - c_1 X_{\beta_1}, \ldots, X_{\alpha_t} - c_t X_{\beta_t}$ of $\mathbf{I_S}(c_1, \ldots, c_t)$. Then f can be written

$$f = \sum_{i=1}^{m_1} a_{i,1} L_{i,1} (X_{\alpha_1} - c_1 X_{\beta_1}) R_{i,1} + \cdots + \sum_{i=1}^{m_t} a_{i,t} L_{i,t} (X_{\alpha_t} - c_t X_{\beta_t}) R_{i,t}$$

where $a_{i,j} \in k, L_{i,j}, R_{i,j} \in \langle x_1, \ldots, x_n \rangle$ for $1 \leq j \leq t$ and $1 \leq i \leq m_j$.

Given such an expression f, we define a directed, vertex-weighted graph G_f with vertex set

$$V(G_f) = \{L_{ij} X_{\alpha_i} R_{ij} | 1 \leq j \leq t, 1 \leq i \leq m_j\} \bigcup \{L_{ij} X_{\beta_i} R_{ij} | 1 \leq j \leq t, 1 \leq I \leq m_j\},$$

and an edge e_{ij} from $L_{ij} X_{\alpha_i} R_{ij}$ to $L_{ij} X_{\beta_i} R_{ij}$ for each i, j such that $1 \leq j \leq t, 1 \leq i \leq n_j$. Note that it is possible to have two different expressions f and f' such that f and f' are equal as polynomials, but $G_f \neq G_{f'}$.

Next we define the weight function w on the vertices of the graph G_f. First, for a pair (v, e) where v is a vertex of G_f and e is an edge of G_f incident to v, we define $w(v, e)$ as

follows:

$$w(L_{ij}X_{\alpha_i}R_{ij}, e_{ij}) = a_{ij}, \text{ and}$$

$$w(L_{ij}X_{\beta_i}R_{ij}, e_{ij}) = -c_j a_{ij}.$$

For a vertex v of G_f, define

$$w(v) = \sum_{\substack{e \text{ incident} \\ \text{with } v}} w(v, e).$$

As a polynomial, then, $f = \sum_{v \in G_f} w(v)v$.

Lemma 3.9 *Suppose $\prec$ is a well ordering of $\mathbf{Z}^t$, f is a polynomial, and a, b, and c are vertices of $\mathbf{G}_f$. Then*

$$\mathrm{g}_\prec(a, c) = \mathrm{g}_\prec(a, b)\mathrm{g}_\prec(b, c). \tag{3.1}$$

Proof. It is clear from the definition of $\mathrm{g}_\prec$ that if any one of $\mathrm{g}_\prec(a, c), \mathrm{g}_\prec(a, b)$, or $\mathrm{g}_\prec(b, c)$ is $\mathbf{0}$, then at least two are, and hence (3.1) is true. Now suppose each element of $\{\mathrm{g}_\prec(a, c), \mathrm{g}_\prec(a, b), \mathrm{g}_\prec(b, c)\}$ is not $\mathbf{0}$. We have:

$$(n_\prec(a, b) + n_\prec(b, c)) \cdot \Delta(S) =$$

$$n_\prec(a, b) \cdot \Delta(S) + n_\prec(b, c) \cdot \Delta(S) = (\hat{\mathbf{x}}(b) - \hat{\mathbf{x}}(a)) + (\hat{\mathbf{x}}(c) - \hat{\mathbf{x}}(b)) =$$

$$\hat{\mathbf{x}}(c) - \hat{\mathbf{x}}(a) = n_\prec(a, c) \cdot \Delta(S).$$

Thus

$$(n_\prec(a, b) + n_\prec(b, c) - n_\prec(a, c)) \cdot \Delta(S) = \mathbf{0},$$

so

$$\mathbf{c}^{n_\prec(a,b)+n_\prec(b,c)-n_\prec(a,c)} = 1,$$

and thus

$$\mathbf{c}^{n_\prec(a,b)}\mathbf{c}^{n_\prec(b,c)} = \mathbf{c}^{n_\prec(a,c)},$$

i.e.,

$$\mathrm{g}_\prec(a,c) = \mathrm{g}_\prec(a,b)\mathrm{g}_\prec(b,c). \quad \blacksquare$$

Lemma 3.10 *Suppose $\prec$ is an effective swo of $\mathbf{Z}^t$, $\mathbf{I_S}(c_1,\ldots c_t)$ satisfies the hypotheses of Theorem 3.7, f is a $k\{x_1,\ldots,x_n\}$-linear combination of the generators $X_{\alpha_1}-X_{\beta_1},\ldots,X_{\alpha_t}-X_{\beta_t}$ of $\mathbf{I_S}(c_1,\ldots,c_t)$, and r is a fixed vertex of $\mathbf{G}_f$. Then*

$$\sum_{v\in G_f} \mathrm{g}_\prec(v,r)w(v) = 0.$$

Proof. Applying the definition of $w(v)$ and reindexing, we obtain:

$$\sum_{v\in G_f} (\mathrm{g}_\prec(v,r)w(v)) = \sum_{v\in G_f} \left((\mathrm{g}(v,r)) \sum_{\substack{e\text{incident}\\ \text{with}v}} w(v,e) \right) =$$

$$\sum_{v\in G_f} \sum_{\substack{e\text{incident}\\ \text{with}v}} (\mathrm{g}_\prec(v,r))\, w(v,e) =$$

$$\sum_{\substack{e \text{ an edge}\\ \text{from } v \text{ to } v'\\ \text{in } \mathbf{G}_f}} (\mathrm{g}_\prec(v,r)w(v,e)) + (\mathrm{g}_\prec(v',r)w(v',e)) \tag{3.2}$$

Applying Lemma 3.9, we see that (3.2) is equal to:

$$\sum_{\substack{e \text{ an edge} \\ \text{from } v \text{ to } v' \\ \text{in } G_f}} g_{\prec}(v,r)\left(w(v,e) + g_{\prec}(v',v)\, w(v',e)\right). \tag{3.3}$$

We now make use of the fact that we have an explicit description of the edges e_{ij} of $\mathbf{G_f}$, which allows us to rewrite (3.3) as:

$$\sum_{j=1}^{t}\sum_{i=1}^{m_j} g_{\prec}(L_{ij}X_{\alpha_i}R_{ij}, r)\left(w(L_{ij}X_{\alpha_i}R_{ij}, e_{ij}) + g_{\prec}(L_{ij}X_{\beta_i}R_{ij}, L_{ij}X_{\alpha_i}R_{ij})w(L_{ij}X_{\beta_i}R_{ij}, e_{ij})\right),$$

which simplifies to:

$$\sum_{j=1}^{t}\sum_{i=1}^{m_j} g_{\prec}(L_{ij}X_{\alpha_i}R_{ij}, r)\left(a_{ij} + g_{\prec}(L_{ij}X_{\beta_i}R_{ij}, L_{ij}X_{\alpha_i}R_{ij}) - c_j a_{ij}\right). \tag{3.4}$$

Finally,

$$\hat{x}(L_{ij}X_{\alpha_i}R_{ij}) - \hat{x}(L_{ij}X_{\beta_i}R_{ij}) = -\Delta(X_{\alpha_j}, X_{\beta_j}) = \overbrace{[0,\ldots,0,-1,0,\ldots,0]}^{\text{-1 in the } j\text{th position}} \cdot \Delta(\mathbf{S}),$$

thus

$$g_{\prec}(L_{ij}X_{\beta_i}R_{ij}, L_{ij}X_{\alpha_i}R_{ij}) = c^{\overbrace{[0,\ldots,0,-1,0,\ldots,0]}^{\text{-1 in the } j\text{th position}}} = c_j^{-1},$$

and (3.4) further simplifies to

$$\sum_{j=1}^{t}\sum_{i=1}^{m_j} g_{\prec}(L_{ij}X_{\alpha_i}R_{ij}, r)\left(a_{ij} + c_j^{-1}\left(-c_j a_{ij}\right)\right). \tag{3.5}$$

Since each summand of (3.5) is 0, we have reached the desired result. ∎

Proof of Theorem 3.7.

(1) Note that f is a monomial if and only if $\mathbf{G}_f$ has exactly one vertex with nonzero weight, and Lemma 3.10 precludes this possibility.

(2) ($\Rightarrow$). Suppose $C_S(X_\alpha) = C_S(X_\beta)$. By Lemma 3.6, there is $\mathbf{n} \in \mathbf{Z}^t$ such that $\mathbf{n}\cdot\Delta(S) = \hat{x}(X_\beta) - \hat{x}(X_\alpha)$ and $X_\alpha - \mathbf{c}^{\mathbf{n}} X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$. Now since $\mathbf{n}_\prec(X_\alpha, X_\beta)\cdot\Delta(S) = \mathbf{n}\cdot\Delta(S)$, we have $(\mathbf{n}_\prec(X_\alpha, X_\beta) - \mathbf{n})\cdot\Delta(S) = 0$, so $\mathbf{c}^{\mathbf{n}_\prec(X_\alpha,X_\beta)-\mathbf{n}} = 1$. Thus $\mathbf{c}^{\mathbf{n}_\prec(X_\alpha,X_\beta)} = \mathbf{c}^{\mathbf{n}}$, so $X_\alpha - \mathbf{c}^{\mathbf{n}_\prec(X_\alpha,X_\beta)} X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$, i.e. $X_\alpha - \mathbf{g}(X_\alpha, X_\beta)X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$.

($\Leftarrow$). Suppose $X_\alpha - \mathbf{g}_{\prec,S}(X_\alpha, X_\beta)X_\beta \in \mathbf{I_S}(c_1, \ldots, c_t)$, and $C_S(X_\alpha) \neq C_S(X_\beta)$. Then by Lemma 3.1, $X_\alpha \in \mathbf{I_S}(c_1, \ldots, c_t)$, contradicting (1) above. ∎

Chapter 4

The single-relator/principal ideal case

The case in which $\mathbf{S}$ is a singleton is of special interest. In the semigroup setting, the *one-relator semigroup word problem*, which asks whether or not there is a singleton set $\mathbf{S}$ such that the one-relator semigroup $\mathbf{M_S}$ has an unsolvable word problem, is still open. The article by Lallement [10] surveys some of the progress that has been made on this problem, including the following result, due to work of S. I. Adjan and G. U. Oganesyan [1, 2, 20]:

Lemma 4.0. *If there is a one-relator semigroup with unsolvable word problem, then there is a one-relator semigroup of the form* $\langle x_1, \ldots, x_n | x_i u x_i = x_j v x_i \rangle$, *where* $u, v \in \langle x_1, \ldots, x_n \rangle$ *and* $i \neq j \in \{1, \ldots, n\}$ *having unsolvable word problem.*

The one relator word problem is related to the membership problem as follows:

Proposition 4.1 *The following are equivalent:*

1. *There is a singleton set* $S \subseteq \langle x_1, \ldots, x_n \rangle^2$ *such that* $\mathbf{G_S}$ *is uncomputable.*
2. *There is a one-relator semigroup with unsolvable word problem.*
3. *There is a principal ideal* $(X_{\alpha_1} - c_1 X_{\beta_1})$ *of* $\mathbf{Q}\langle x_1, \ldots, x_n \rangle$, *with* $c_1 \neq 0$, *having unsolvable membership problem.*

Proof. 1 $\iff$ 2. Corollary 3.8.

2 $\iff$ 3. Remark 1 (after Corollary 3.8) and Corollary 3.8. ∎

In this chapter, we introduce some ideas of particular relevance to the one-relator/principal ideal case. In section 4.1, *weights* are introduced and used to show that certain of the semigroups $\langle x_1, \ldots, x_n | x_i u x_i = x_j v x_i \rangle$ $(i \neq j)$ have a solvable word problem. The notion of $\mathcal{P}$-computability with respect to a partition $\mathcal{P}$ of the monomials is introduced in Section 4.2.

4.1 WEIGHTS

Definition. A *weight* is a homomorphism from the multiplicative semigroup $\langle x_1, \ldots, x_n \rangle$ into the additive semigroup of integers $(\mathbf{Z}, +)$. Thus any assignment of integers to the variables determines a weight. A weight w is *positive* if $w(x_t) > 0$ for each $t, 1 \leq t \leq n$.

Recall $\hat{x}_i(m)$ denotes the number of x_i's appearing in the monomial m. Thus, for any weight $w : \langle x_1, \ldots, x_n \rangle \to \mathbf{Z}$ and for any monomial $m \in \langle x_1, \ldots, x_n \rangle$,

$$w(m) = \sum_{t=1}^{n} w(x_t)\hat{x}_t(m).$$

Theorem 4.2 *Suppose* $S = \{(X_{\alpha_1}, X_{\beta_1})\} \subseteq \langle x_1, \ldots, x_n \rangle^2$. *If there is a positive weight* w *such that* $w(X_{\alpha_1}) = w(X_{\beta_1})$, *then* $\mathbf{G}_S$ *is computable.*

Proof. Suppose w is a positive weight and $w(X_{\alpha_1}) = w(X_{\beta_1})$. We have $w(r) = w(s)$ for each pair (r, s) of adjacent vertices of $\mathbf{G_S}$ and thus $w(r) = w(s)$ whenever there is a

path from r to s in $\mathbf{G_S}$. Thus, for each component C of $\mathbf{G_S}$, there is a positive integer a such that $w(m) = a$ whenever $m \in C$, i.e.

$$\sum_{t=1}^{n} w(x_t)\hat{x}_t(m) = a \text{ for each } m \in C. \tag{4.1}$$

Since $w(x_1), \ldots, w(x_n)$, and a are all positive, (4.1) has at most finitely many solutions for $\hat{x}_1(m), \ldots, \hat{x}_n(m)$ in the positive integers. Thus each component C of $\mathbf{G_S}$ is finite. For monomials X_α, X_β, then, it is possible to enumerate $C_S(X_\alpha)$ and $C_S(X_\beta)$ in finite time and thus determine whether or not $C_S(X_\alpha) = C_S(X_\beta)$. ∎

Before proving Corollary 4.4, we prove for the sake of completeness the following simple but useful lemma.

Lemma 4.3 *Suppose $m_1, \ldots, m_n$ are nonzero integers. If $m_j > 0$ and $m_k < 0$ for some $j, k \in \{1, \ldots, n\}$, then the equation*

$$\sum_{i=1}^{n} m_i x_i = 0 \tag{4.2}$$

has a solution $x_1 = \bar{x}_1, \ldots, x_n = \bar{x}_n$ in the positive integers.

Proof. We proceed by induction on n, the base case being $n = 2$. In this case, we may assume that $m_1 > 0$ and $m_2 < 0$ Then, choosing $\bar{x}_1 = -m_2, \bar{x}_2 = m_1,$, we have $\bar{x}_1 > 0, \bar{x}_2 > 0$, and $m_1\bar{x}_1 + m_2\bar{x}_2 = 0$. Now assume that if $m_j > 0$ and $m_k < 0$ for some $j, k \in \{1, \ldots, n\}$, then equation (4.2) has a solution in the positive integers, and assume $m_1, \ldots, m_{n+1}$ are nonzero integers with $\text{sign}(m_n) \neq \text{sign}(m_{n+1})$. The equation

$$\sum_{i=1}^{n} m_i x_i = 0$$

has a solution $x_1 = \bar{x}_1, \ldots, x_n = \bar{x}_n$ consisting of positive integers by the induction hypothesis. If $m_n < 0$ and $m_{n+1} > 0$, then $x_1 = \bar{x}_1, \ldots, x_{n-1} = \bar{x}_{n-1}, \bar{x}_n = \bar{x}_n + m_{n+1}, x_{n+1} = -m_n$ is a positive integer solution to

$$\sum_{i=1}^{n+1} m_i x_i = 0. \tag{4.3}$$

On the other hand, if $m_n > 0$ and $m_{n+1} < 0$, then $x_1 = \bar{x}_1, \ldots, x_{n-1} = \bar{x}_{n-1}, x_n = \bar{x}_n - m_{n+1}, x_{n+1} = m_n$ is a positive integer solution of (4.3). ∎

Corollary 4.4 *Suppose* $S = \{(X_{\alpha_1}, X_{\beta_1})\}$. *If there exist* $i, j \in \{1, \ldots, n\}$ *such that:*

1. $\hat{x}_i(X_{\alpha_1}) > \hat{x}_i(X_{\beta_1})$ *and* $\hat{x}_j(X_{\alpha_1}) < \hat{x}_j(X_{\beta_1})$, *or*
2. $\hat{x}_i(X_{\alpha_1}) < \hat{x}_i(X_{\beta_1})$ *and* $\hat{x}_j(X_{\alpha_1}) > \hat{x}_j(X_{\beta_1})$,

then $\mathbf{G_S}$ *is computable.*

Proof. To show that $\mathbf{G_S}$ is computable, it suffices by Theorem 4.2 to show that there is a positive weight w such that $w(X_{\alpha_1}) = w(X_{\beta_1})$. This is true if and only if there are positive integers $w(x_1), \ldots, w(x_n)$ such that

$$\sum_{t=1}^{n} \hat{x}_t(X_{\alpha_1}) w(x_t) = \sum_{t=1}^{n} \hat{x}_t(X_{\beta_1}) w(x_t),$$

$$\text{i.e., } \sum_{t=1}^{n} \left(\hat{x}_t(X_{\alpha_1}) - \hat{x}_t(X_{\beta_1})\right) w(x_t) = 0. \tag{4.4}$$

If either hypothesis (1) or (2) is satisfied, (4.4) has at least one solution for $w(x_1), \ldots, w(x_n)$ in the positive integers by Lemma 4.3. ∎

In particular, the proof of Corollary 4.4 shows that if $\mathbf{S}$ satisfies the hypotheses of the corollary, then each component of $\mathbf{G_S}$ is finite. A similar result is proven in [25].

Corollary 4.5 *If there is a one-relator semigroup with unsolvable word problem, then there is a semigroup* $\langle x_1, \ldots, x_n | X_{\alpha_1} = X_{\beta_1} \rangle$ *having unsolvable word problem, where* X_{α_1} *and* X_{β_1} *have the same initial letter and different terminal letters, and:*

1. $\hat{x}_t(X_{\alpha_1}) \leq \hat{x}_t(X_{\beta_1})$ *for each* $t \in \{1, \ldots, n\}$, *or*

2. $\hat{x}_t(X_{\alpha_1}) \geq \hat{x}_t(X_{\beta_1})$ *for each* $t \in \{1, \ldots, n\}$.

Proof. Corollary 4.4 and Lemma 4.0. ∎

4.2. PARTITIONS

A *partition* of $\langle x_1, \ldots, x_n \rangle$ is a collection $\mathcal{P} = \{P_1, P_2, \ldots\}$ of nonempty subsets of $\langle x_1, \ldots, x_n \rangle$ satisfying:

(i) $P_i \bigcap P_j = \phi$ whenever $i \neq j$

(ii) $\bigcup_{i=1}^{\infty} P_i = \langle x_1, \ldots, x_n \rangle$.

The sets $P_1, P_2, \ldots$ comprising the partition are the *cells* of $\mathcal{P}$.

Examples

1. Suppose w is a weight. Those sets $w^{-1}(i), i \in \mathbf{Z}$ that are nonempty form a partition, denoted $\mathcal{P}(w)$.

2. For non-negative integers $a_1, \ldots, a_n$, let $\mathbf{a} = [a_1, \ldots, a_n] \in \mathbf{N}^n$, and let $C_{\mathbf{a}} = \{m \in \langle x_1, \ldots, x_n \rangle | \hat{x}_i(m) = a_i \text{ for each } i \in \{1, \ldots, n\}\}$. The collection $\mathcal{C} = \{C_{\mathbf{a}} | \mathbf{a} \in \mathbf{N}^n\}$ forms a partition of $\langle x_1, \ldots, x_n \rangle$.

3. Suppose $Q_0 \subseteq \langle x_1, \ldots, x_n \rangle$ is such that Cardinality$(Q_0 \bigcap C) = 1$ for each component C of $\mathbf{G_S}$. Let $Q_i = \{p | d(p, Q_0) = i\}$. The collection $\mathcal{Q} = \{Q_0, Q_1, \ldots\}$ forms a partition.

Recall that a graph $\mathbf{G_S}$ on $\langle x_1, \ldots, x_n \rangle$ is computable if there is an algorithm which determines whether or not two arbitrary words are in the same component of G.

Definition. Suppose $\mathcal{P} = \{P_1, P_2, \ldots\}$ is a partition of $\langle x_1, \ldots, x_n \rangle$ and $\mathbf{G_S}$ is a graph on the monomials. $\mathbf{G_S}$ is *$\mathcal{P}$-computable* if there is an algorithm that determines whether or not two words from the same $\mathcal{P}$-cell are from the same component of $\mathbf{G_S}$, i.e. $\mathbf{G_S}$ is $\mathcal{P}$-computable if there is an algorithm which solves each instance of the following problem:

INSTANCE: $X_\alpha, X_\beta \in \langle x_1, \ldots, x_n \rangle$ such that X_α and X_β are from the same cell of $\mathcal{P}$.

PROBLEM: Determine whether or not $C_S(X_\alpha) = C_S(X_\beta)$.

The following theorem involves Example 2 above.

Theorem 4.6 *Suppose $S = \{(X_{\alpha_1}, X_{\beta_1})\}$. The following are equivalent:*

1. $\mathbf{G}_S$ *is $\mathcal{P}(w)$-computable for some weight w.*
2. $\mathbf{G}_S$ *is $\mathcal{C}$-computable.*
3. $\mathbf{G}_S$ *is computable.*

The proof requires a preliminary observation.

Lemma 4.7 *Suppose $S = \{(X_{\alpha_1}, X_{\beta_1})\} \subseteq \langle x_1, \ldots, x_n \rangle^2$ and X_α and X_β are adjacent vertices of $\mathbf{G_S}$. Let $\mathbf{u}_1 = \hat{\mathbf{x}}(X_{\beta_1}) - \hat{\mathbf{x}}(X_{\alpha_1})$. If $X_\alpha \in C_{\mathbf{a}}$, then $X_\beta \in C_{\mathbf{a}+\mathbf{u}_1}$ or $X_\beta \in C_{\mathbf{a}-\mathbf{u}_1}$.*

This lemma makes it clear that, when $\mathbf{S}$ is a singleton, $\mathbf{G_S}$ cannot have an odd cycle,

and thus must be bipartite. Also, if $C_S(X_\alpha) = C_S(X_\beta)$, where $X_\alpha \in C_{\mathbf{a}}, X_\beta \in C_{\mathbf{b}}$, then $\mathbf{a} - \mathbf{b} \in \{n\mathbf{u}_1 | n \in \mathbf{Z}\}$.

Proof of Theorem 4.6.

($1 \Rightarrow 2$.) Suppose $\mathbf{G}_S$ is w-computable for a weight w, so there is an algorithm $\mathcal{A}$ that determines whether or not two words with the same weight are in the same component of $\mathbf{G}_S$. If r and s are from the same cell of $\mathcal{C}$, then $w(r) = w(s)$ and the algorithm $\mathcal{A}$ can be applied to determine whether or not r and s are in the same component of $\mathbf{G}_S$.

($2 \Rightarrow 3$.) Suppose now that $\mathcal{B}$ is an algorithm that determines whether or not two words from the same $\mathcal{C}$-cell are in the same component of $\mathbf{G}_S$, and suppose X_α and X_β are vertices of $\mathbf{G_S}$ with $X_\alpha \in C_{\mathbf{a}}$ and $X_\beta \in C_{\mathbf{b}}$. Let $\mathbf{u}_1 = \hat{\mathbf{x}}(X_{\beta_1}) - \hat{\mathbf{x}}(X_{\alpha_1})$. If $\mathbf{a} - \mathbf{b} \notin \{n\mathbf{u}_1 | n \in \mathbf{Z}\}$, then $C_S(X_\alpha) \neq C_S(X_\beta)$, by Lemma 4.7. Otherwise, we may assume without loss of generality (by swapping X_α and X_β if necessary) that there is a *positive* integer n such that $\mathbf{b} = \mathbf{a} + n\mathbf{u}_1$.

Claim. $C_S(X_\alpha) = C_S(X_\beta) \iff$ there is a path Q in $\mathbf{G_S}$ satisfying the following:

1. origin$(Q) = X_\alpha$,
2. terminus$(Q) \in C_{\mathbf{b}}$,
3. For each vertex v of Q,we have $v \in C_{\mathbf{a}+m\mathbf{u}_1}$, for some $m \leq n$,
4. C_S(terminus $(Q)) = C_S(X_\beta)$.

Proof of Claim.

($\Rightarrow$). Suppose $C_S(X_\alpha) = C_S(X_\beta)$ and $P = (X_\alpha = p_0, p_1, \ldots, p_l = X_\beta)$ is a path from X_α to X_β in $\mathbf{G_S}$. Let $j = \min\{i | p_i \in C_{\mathbf{b}}\}$. The path $Q = (p_0, p_1, \ldots, p_j)$ clearly satisfies (1) and (2). Also, Q satisfies (3) (by Lemma 4.7 and the definition of j), and (4) (since $C_S(X_\alpha) = C_S(X_\beta)$ by hypothesis.)

($\Leftarrow$). Suppose Q is a path in $\mathbf{G_S}$ satisfying (1), (2), (3), and (4). Then $C_S(X_\alpha) = C_S(\text{terminus}(Q)) = C_S(X_\beta)$. This completes the proof of the claim.

Now let $\mathcal{T} = \{\text{paths } \mathcal{Q} \text{ in } \mathbf{G_S} | \mathcal{Q} \text{ satisfies (1), (2), (3), and (4)}\}$. The set of paths in $\mathbf{G_S}$ satisfying (3) is finite and computable, and thus $\mathcal{T}$ is also finite and computable, since conditions (1), (2), and (4) are decidable ((1) and (2) by inspection and (4) by hypothesis). By the claim, we have

$$C_S(X_\alpha) = C_S(X_\beta) \iff \mathcal{T} \neq \phi.$$

Since the condition $\mathcal{T} \neq \phi$ is decidable, the condition $C_S(X_\alpha) = C_S(X_\beta)$ is also decidable. Thus $\mathbf{G_S}$ is computable.

(3 $\Rightarrow$ 1.) This implication is clear. ∎

Bibliography

[1] S.I. Adjan, G.U. Oganesyan, *On the word and divisibility problems in semigroups with a single defining relator.* Izv. Akad. Nauk SSSR, Ser. Mat., 42, no. 2 (1978), 219 -225 (Russian).

[2] S.I. Adjan, G.U. Oganesyan, *On the word and divisibility relation problems for semigroups with one relation.* Mat. Zametki, 41, no. 3, (1987), 412 -421 (Russian).

[3] K. Appel, *Small Cancellation Theory or What I Once Did for a Living*, manuscript, University of New Hampshire.

[4] D. Bayer, M. Stillman, *On the Complexity of Computing Syzygies.* Computational aspects of commutative algebra. J. Symbolic Comput. 6 (1988), no. 2-3, 135–147.

[5] G. M. Bergman, *The diamond lemma for ring theory.* Adv. in Math 29 (1978), no. 2, 178 - 218.

[6] D. Collins, *Peak Reduction and Automorphisms of Free Groups and Free Products*, Combinatorial Group Theory and Topology (Alta, Utah, 1984), 107 - 120, Ann. of Math. Stud. 111, Princeton Univ. Press, Princeton, N.J., 1987.

[7] M. Dehn, *Uber die Topologie des dreidimensionalen Raumes.* Math. Ann., 69, 137 - 168, 1910.

[8] M. Dehn, *Uber unendliche diskontinuierliche Gruppen.* Math. Ann., 71, 116 - 144, 1911.

[9] D. Eisenbud, I. Peeva, B. Sturmfels, *Non-commutative Grobner bases for commutative algebras.* Proc. Amer. Math. Soc., 126, no. 3, 687 - 691, 1998.

[10] G. Lallement, *The Word Problem for Thue Rewriting Systems.* Term rewriting (Font Romeux, 1993), 27–38, Lecture Notes in Computer Science, 909, Springer, Berlin, 1995.

[11] W. Magnus. *Das Identitats problem fur Gruppen mit einer definierenden Relation.* Math Ann., 106: 295 - 307, 1932.

[12] A.A. Markov, *Impossibility of certain algorithms in the theory of associative systems.* Dokl. Akad. Nauk. SSSR, 55(7):587 - 590, 1947.

[13] Y. Matiyasevich, *Simple examples of undecidable associative calculi.* Dokl. Akad. Nauk SSSR 173: 1264 - 1266, 1967.

[14] Y. Matiyasevich, *Word Problem for Thue Systems with a Few Relations.* Term Rewriting (Font Romeux, 1993), 39 - 52, Lecture Notes in Computer Science, 909, Springer, Berlin, 1995.

[15] F. Mora, *Groebner Bases for Non-commutative polynomial rings.* Algebraic algorithms and error correcting codes (Grenoble, 1985), 353 - 362, Lecture Notes in Computer Science, 229, Springer, Berlin.

[16] T. Mora, *An introduction to commutative and noncommutative Grobner bases.* Theoretical Computer Science 134: 131 - 173, 1994.

[17] T. Mora, *Grobner bases and the word problem.* Working Paper, Genova, 1987.

[18] K. Madlener, B. Reinert, *Relating rewriting techniques on monoids and rings: congruences on monoids and ideals in monoid rings.* Theoretical Computer Science 208: 3 - 31, 1998.

[19] M. H. A. Newman, *On Theories with a Combinatorial Definition of "Equivalence"*, Ann. Math. 43, no. 2 (1942) 223 - 243.

[20] G. U. Oganesyan, *On the problems of equality and divisibility of words in a semigroup with a defining relation of the form* $a = bA$. Iav. Akad. Nauk. SSR, Ser. Mat., 42 no. 3 (1978), 602 - 612 (Russian).

[21] E. L. Post, *Recursive unsolvability of a problem of Thue.* J. Symbolic Logic, 12: 1 -11, 1947.

[22] F. L. Pritchard, *The ideal membership problem in non-commutative polynomial rings.* J. Symbolic Computation, 22, no.1: 27 - 48 (1996).

[23] C. Squier, *Word Problems and a Homological Finiteness Condition for Monoids.* J. Pure Appl. Algebra, 49, 201 - 217 (1987).

[24] A. Thue, *Probleme uber Veranderungen von Zeichenreihen nach gegebenen Regeln.* Skrifter utgit av Videnskapsselskapet i Kristiania, I. Matematisk-naturvidenskabelig klasse, 10, 34 pp., 1914. Reprinted in: A. Thue. Selected Mathematical Papers. Oslo, 1977, 493 - 524.

[25] A. Yasuhara, *The Solvability of the Word Problem for Certain Semigroups.* Proc. Amer. Math. Soc. 26 (1970), 645 -650.